```
VZCZCXRO9778
OO RUEHAG RUEHAST RUEHDA RUEHDBU RUEHDF RUEHFL RUEHIK RUEHKW RUEHLA
RUEHLN RUEHLZ RUEHMRE RUEHNP RUEHPOD RUEHROV RUEHSK RUEHSR RUEHVK
RUEHYG
DE RUEHVEN #0064/01 0841606
ZNR UUUUU ZZH
O 251606Z MAR 09
FM USMISSION USOSCE
TO RUEHC/SECSTATE WASHDC IMMEDIATE 6278
INFO RUCNCFE/CONVENTIONAL ARMED FORCES IN EUROPE PRIORITY
RUEHNO/USMISSION USNATO PRIORITY 1718
RUEAIIA/CIA WASHDC PRIORITY
RUEKJCS/DIA WASHDC PRIORITY
RUEKJCS/SECDEF WASHDC PRIORITY
RUESDT/DTRA-OSES DARMSTADT GE PRIORITY
RHMFISS/CDR USEUCOM VAIHINGEN GE PRIORITY
RUEKJCS/JOINT STAFF WASHDC//J5-DDPMA-IN/CAC/DDPMA-E// PRIORITY
RUEAHQA/HQ USAF WASHINGTON DC//XONP// PRIORITY
RUEADWD/DA WASHINGTON DC PRIORITY
RUEASWA/DTRA ALEX WASHINGTON DC//OSAE PRIORITY
RUEHZL/EUROPEAN POLITICAL COLLECTIVE 0080
RUCNOSC/OSCE COLLECTIVE
```

UNCLAS SECTION 01 OF 07 USOSCE 000064

SENSITIVE
SIPDIS

STATE FOR VCI/CCA, EUR/RPM, NSA FOR STANAR-JOHNSON, T FOR
KATSAPIS, OSD EUR/NATO, OSD/NII FOR HALL, DHS FOR DENNING,
NSC FOR HATHAWAY, NSC FOR DONAHUE, NSC FOR CUMMINGS, WINPAC
FOR FRITZMEIER, ISN FOR KARTCHNER,
NSC FOR HAYES
JCS FOR J5/COL NORWOOD
OSD FOR ISA (PERENYI)

E.O. 12958: N/A
TAGS: EINT FR KCFE KHLS OSCE PARM PREL RS KCIP
SUBJECT: OSCE/FSC: DAY ONE--OSCE WORKSHOP ON A
COMPREHENSIVE OSCE APPROACH TO ENHANCING CYBERSECURITY

¶1. (U) NOTE: This is the first of two cables reporting the March 17-18 OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cybersecurity. END NOTE.

¶2. (SBU) Summary: More than 200 civil and military representatives gathered in Vienna, March 17) 18, in the first wide-scale FSC effort to discuss cybersecurity. This was one of the more broadly attended workshops held under the auspices of the OSCE, with reps in attendance from Egypt, Japan, the Arab League, and NATO, among others. Their key aim was to identify ways to cooperate on enhancing cybersecurity and examine the potential future role of the OSCE in addressing this global problem. Washington reps, led by State/INR Michele Markoff, also consisted of reps from State/EEB, DHS, and DOD.

¶3. (SBU) Initially considered by the U.S. a risky topic for the FSC, the workshop proved a successful endeavor for achieving U.S. objectives, which were to prevent the militarization of cyber security, refrain from engaging in discussions on constraining state capabilities, and keeping the focus on defensive remedies to ensure cyber security. There was much support for the U.S. position to focus on defensive strategies and for a U.S. recommendation that OSCE participating States conduct a self-survey to identify gaps and capacities in order to later devise an approach to cyber resiliency. There was very little support for Russia's description of cyber security as an "information arms race" that required a new international treaty instrument. Russia's proposal to begin by defining relevant terms and concepts also gained little traction. Russia was alone in its opposition to the Council of Europe Convention on Cyber Crime. Turkey reported that inconsistencies with its own national legislation had kept it from adopting the convention, but asked USdel on the margins of the workshop for assistance in reconciling this obstacle.

¶4. (SBU) There was strong support for U.S. expert participation from Washington in the workshop. Several delegations praised the efforts of the U.S. panelists (State/INR, DOD, and DHS reps) and pointed out the U.S. rep's excellent job of summarizing two days of discussion in the last working session. Several delegations were eager to follow up with the U.S. head of del after her presentation. EU reps invited U.S. participation/expertise to an informal ministerial conference on critical information infrastructure protection (CIIP), to be held April 27-28 in Tallinn. A number of possible recommendations for follow-up activities were proposed. We would welcome Washington guidance on how it envisions follow-up activity in Vienna.

¶5. (SBU) COMMENT: If the USG wishes to move forward on cyber security in the OSCE, a new CSBM introduced by the U.S. and close Allies on cyber security may be in U.S. interest for three reasons. First, this could advance the U.S. approach with the 56 participating States (pS), over half of whom are not in NATO. Second, this would proactively offer a positive alternative to displace unhelpful Russian proposals and prevent Russian views from being the center of attention. Third, the U.S. would assert leadership. Such a CSBM could be centered, for instance, around the 6-7 well-received recommendations the USG panelist made at the end of the workshop or the 11 agreed points on cyber security already agreed within the G-8. By moving forward with one of the recommendations that were also proposed in the non-paper authored by Austria, Estonia, and Lithuania, the U.S. could enlist one or all of these countries as co-leads of the action. END COMMENT.

END SUMMARY.

- -
Opening Session: OSCE Takes on Cyber security
- -

¶6. (U) Greek Chairman in Office (Ambassador Mara Marinaki) opened the March 17 -18 OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security by saying it was the first wide-scale OSCE effort to discuss cyber security, building on previous OSCE efforts to combat terrorism on the Internet, exchange information, and discuss concrete steps for a way forward. The Greek CiO pointed out, in particular, a jointly sponsored non-paper authored by Austria, Estonia, and Lithuania (FSC.DEL/33/09), which lays out specific concerns related to cyber security and a possible way forward for the OSCE to address those concerns. The OSCE Secretary General Marc Perrin de Brichambaut commented that the holding of this event demonstrated how the OSCE was seeking to remain in step with modern-day challenges. Cyber security as a theme also showed continued relevance of the OSCE's signature concern of "comprehensive security." The SYG hoped the workshop could explore what kind of comprehensive approach the OSCE could craft and how could it help participating States. He said that OSCE pS had been working to create a mandate to enhance cyber security by (1) combating terrorist use of the Internet (MC.DEC/3/04 and MC.DEC/7/06); (2) promoting public-private partnerships (MC.DEC/5/07); and (3) crafting a comprehensive OSCE approach to cyber security (FSC.DEC/10/08).

¶7. (SBU) The Estonian Minister of Defense Jaak Aaviksoo called cyber security an "essential and demanding" topic (FSC.DEL/42/09). He saw the OSCE as an ideal forum for this discussion given the need for "security and cooperation in Europe" on cyber security and also called it a "key forum" for discussing a "true 21st century challenge." Aaviksoo stressed the responsibility of pS to raise awareness and described the OSCE as a large intergovernmental organization with a significant role to play. He said a dual approach that would increase cooperation multilaterally and improve resilience on a national basis was needed. He also stressed the need for States to create the national legal framework necessary for a comprehensive cyber security program, and the need for national Computer Emergency Response Teams. More evenly regulated national cyber environments, he said, would contribute to a better governed international space. Aaviksoo also applauded the Council on Europe Convention on Cybercrime as a great framework for cooperation. The Czech Republic (Reinohlova) on behalf of the European Union said that cyber security was an "important precondition" for defending values.

Session 1: Threats to Cyber security

¶8. (SBU) The first session addressed attributes and common forms of cyber attacks, cyber crime, defensive strategies for threat mitigation, and consequence management and remediation. Keynote speakers were Captain H.N. Dionisis Antonopolous, Director Cyber Defense Directorate, Hellenic National Defense General Staff; Vladislav Sherstyuk, Deputy Secretary of the Security Council of the Russian Federation; Michele Markoff, Acting Director, Office of Cyber Affairs, Department of State; and Rytis Rainys, Head of Network and Information Security Division of Lithuania. The panel was moderated by Raphael Perl from the Office of the OSCE Secretary General, Action Against Terrorism Unit.

USOSCE 00000064 003 OF 007

Don't Forget the End-User

¶9. (SBU) Antonopolous' presentation, The Key to an Effective Cyber Defense Strategy, focused on the human factor in cyber security (FSC.DEL/38/09). Due to the nature of cyber attacks the end-user often becomes an unknowing victim. He said that most public and private entities provide high level training for cyber security personnel, but it can never be enough. He stressed that the common end-user has been left out and more education for individuals, who use computers daily at home and work, was needed.

Russians Claim New Arms Race Unfolding

¶10. (SBU) Sherstyuk's presentation, Problems of Ensuring International Information Security, made attempts to assert that an "information arms race" was unfolding internationally (FSC.DEL/22/09). He stressed the need for collective action to prevent the "next round of an arms race," claiming that 120 nations had "departments" dealing with cyber warfare. Sherstyuk also believed that it was especially important to draw up a universal document under international law that acknowledged the existence of political-military and criminal threats, including terrorism, to "international information security." He proposed the publication of a dictionary of terms "used in the international information security field." Sherstyuk also mentioned that an international conference on cybercrime jointly sponsored by Russia and Germany would take place on April 18 in Germany.

U.S. Focus on Defense

¶11. (SBU) Markoff's presentation, U.S. Views on National and International Approaches to Information Network Security, focused on securing networks through layered defenses that are effective whatever the source of the attack (FSC.DEL/40/09/Rev.1). Markoff explained that a national review of cyber policy currently was being conducted in Washington and without prejudging the outcome said that the U.S. will continue actively to pursue international collaboration on cyber security in bilateral, multilateral, and international venues. The U.S. would also continue to offer its detailed views of those steps that states, individually and collectively, need to take to enhance cyber security.

¶12. (SBU) Markoff said that cyber security was not inherently political-military in nature, just as information technology is neither inherently civil nor military. Therefore, cyber security was a shared responsibility of government, industry, and individual citizens. Markoff demonstrated that the Russian rep's call for an arms control-like convention that would ban the development or use of a wide range of information technologies was not helpful or effective in addressing the security threats associated with this technology. It also was most likely unenforceable.

Lithuania: "Think Globally, Act Locally"

¶13. (SBU) Rainys' presentation, Overview of Cyber-related Security Incidents in 2008, stressed that cyber attacks were becoming massive and well-organized. He stated that most cyber attacks were motivated by financial gain. His message

was to "think globally, act locally." Rainys said that if each nation could implement an incident management system that would keep its local network as clean as possible, this would, in turn, enhance the security of global networks. Rainys stressed that defensive activities were key. He said that incident management work by CERT groups should be enhanced, technical solutions that could be implemented by network providers would lead to better protection of end-users, and wider cooperation and coordination were important.

Self-Survey As First Step

¶14. (SBU) In response to questions posed by the audience, Markoff suggested that the OSCE first set up a "self-survey" in order to know the gaps and capacities among OSCE pS. Then, Markoff said, the OSCE could design a program where the first steps would be to develop confidence and trust. She also indicated that this could include identifying points of contact for the first responders of member States. Finland (Kangaste) agreed that cyber security posed challenges to all stakeholders and supported defensive measures as the most concrete way for dealing with cyber attacks. He called the Council of Europe Convention on Cyber Crime "groundbreaking." He also echoed the U.S. (Markoff) point about the need to build a "culture of cyber security" as well as the U.S. recommendation for a self-survey. Kangaste said it was important to ensure that the rules of international humanitarian law apply and said that Sweden, Switzerland, and Finland have an ongoing joint study to define what this means for cyber space.

U.S. Upholds Principles of Free Speech

¶15. (SBU) Cyprus agreed with Rainys, statement, "think globally, act locally," but reordered the priority to acting locally and collaborating internationally. The Cyprus rep stressed the need for a well-defined plan and said "perfect planning prevents pathetic performance." Azerbaijan (Jafarova) noted that networks should not be used for "racism, terrorism, or other phobias, such as Islamaphobia." Jafarova spoke about the potential for a state to develop propaganda against another state and said that Azerbaijan had found websites that challenged its territorial integrity and sovereignty. The U.S. (Markoff) responded that while we may witness speech that is hostile and political on the internet, it remains the U.S. position that one's view of illegitimate speech is another's legitimate political expression. In upholding the right of free speech, Markoff cautioned against "regulating content8 and stressed the importance of maintaining the principles of the Universal Declaration of Human Rights.

Russia Says It's Misunderstood; Quotes Castro

¶16. (SBU) Georgia (Kvanchakhadze) recalled the "most serious attack against (their) infrastructure" in August 2008 and questioned who would be the main international body to fight state sponsored attacks. The U.S. (Markoff) stressed that the unique attributes of this technology made the problem of acting against perceived perpetrators very difficult and that a better understanding of the technical issues in the international environment was essential before strategizing further. Russia (Krutskikh) alleged that there was a problem

understanding each other because cyber terms had not been defined. He then said Russia was misunderstood as pushing for "disarmament." Krutskikh said we should use the experience we have already acquired but we should be sure we were targeting the right problems, such as crime, terrorism, and armed attack. He quoted Fidel Castro, who said "if you devise an imaginary enemy, you ignore the real enemy that exists."

¶17. (SBU) Antonopolous tried to clarify that cyber meant the "space where we are when we are talking on the phone." In other words, it is "the non-visual space where you can apply visual actions." The U.S. (Markoff) responded that Krutskikh's comments seemed to imply a change in the Russian position that has held for several years that an arms control race in unfolding. Markoff said that the Russian position had been to establish boundaries of sovereignty in cyber space, but if that had changed, the U.S. would welcome hearing more details.

Session 2: Government Options

¶18. (U) The second session addressed national and international good practices and legal frameworks and their use to develop policy options for governments. Michele Markoff was the moderator. Keynote speakers included John Denning, Director for External Affairs in the Office of Cyber security and Communications, Department of Homeland Security; Patrick Pailloux, Director of Information Security, French General-Secretariat for National Defense; and, Andrea Servida, Directorate General Information Society of the European Commission.

U.S. Describes Cybersecurity Culture

¶19. (SBU) Denning (Department of Homeland Security) called for the construction of a culture of cyber security based on shared responsibility (FSC.DEL/44/09/Add.1). Denning described the key elements of a viable cyber security program as: development of national strategy; collaboration between national governments and industry; deterrence of cybercrime; creation of national incident management capabilities; and promotion of a national culture of cyber security.

¶20. (SBU) Denning said governments must provide an example of good cyber security practices in their outreach to the private sector. He noted that government efforts are inherently multi-agency and, in the U.S., include federal, state, and local officials. His own agency, Homeland

Security, had developed a National Infrastructure Protection Plan that relied on close relationships between the government and key sectors of the critical infrastructure. Inculcating cyber security awareness in all parts of the society will require constant awareness raising and education.

- - - - - - - - - - - - - -

French National Responses

- - - - - - - - - - - - - -

¶21. (SBU) Pailloux said that much thinking in the French government on cyber security was captured in its recent white paper on defense (FSC.DEL/45/09). France, noting the 2007 attack on Estonia, estimates a high probability of cyber attack as the technology required is readily available to many and can be employed with minimal risk to the attacker. He noted that critical infrastructures worldwide increasingly depend on information technology for effective functioning, increasing the risk cyber attacks could seriously impede delivery of vital services to citizens. Pailloux praised the FSC workshop as a necessary effort to raise awareness of the threats to cyber security. Also needed was international agreement on a minimum level of rules and good practices that system operaters need to follow. He also stressed that security requirements should not hamper innovation and rapid technology development in the IT industry, and said that international cooperation is essential to deter and prosecute cybercrime. He said that the EU must take steps to protect its critical information infrastructure, as it protects its other critical infrastructures. The French government CERT, which Pailloux heads, was able to close down over 2,000 phishing sites with the help of its international partners.

- - - - - - - - - - -

EU Policy Initiatives

- - - - - - - - - - -

¶22. (SBU) Andrea Servida described ongoing EU efforts to enhance cyber security in the EU's Member States and institutions. While EU executive agencies like the European Network and Information Security Agency are raising awareness and fostering dialogue with industry, there was also a need for greater public participation in shaping an enhanced European policy on network and information security. The Commission launched an on-line public consultation in 2008 to which academics, industry experts, and private citizens have contributed.

¶23. (SBU) Noting the increasing number and severity of cyber attacks and their costs to national and regional economies, Servida said the Commission had several policy initiatives designed to ensure the protection and survival of European Critical Information Infrastructure. These would be based on both government and private sector programs and would protect against all threats. Next steps include an informal ministerial meeting on critical information infrastructure protection (CIIP) in Tallinn in late April. He noted that while there are 150 CERTs in the EU, only 15 are national-level, of which seven have standard operating language to communicate with each other.

¶24. (SBU) Italy (Somma), in response, described briefly its MOD cyber defense organization and highlights of a recent cyber exercise ("CYBER SHOT") that involved all the military services, including the Carabinieri or national police, and representatives of civilian government agencies and critical information infrastructure. Somma spoke of the importance of setting up a clear command structure for dealing with incidents as they occur, and situational awareness of the state of network defenses. Another exercise is planned in November in conjunction with a NATO cyber event. The Arab League (Wehbe) said it was taking steps to follow UN measures. Wehbe pointed out that the Arab countries were trying to combat terrorist use of the internet while maintaining respect for human rights.

Meridian Process: Connecting Policymakers

¶25. (SBU) The UK (Burnett) described the Meridian Process, which began in 2005 with the support of the EU and G8 for policymakers involved in CIIP. Burnett noted that the Meridian Process is an annual conference, with a rotating presidency, open to any country that wants to join. It had been deemed successful by participants. The presidency was held by the UK (2005), Hungary (2006), Sweden (2007), Singapore (2008), this year (November) by the U.S., and in 2010 by Taiwan. The theme of Meridian is "connecting and protecting," and identify points of contacts between participants. Burnett stressed the conference was meant for policymakers, not CERT professionals or technical experts.

¶26. (U) This cable has been cleared by INR/CCT Markoff; OSD/NII; and, OSD/P.
NEIGHBOUR